PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-111729
(43)Date of publication of application : 12.04.2002

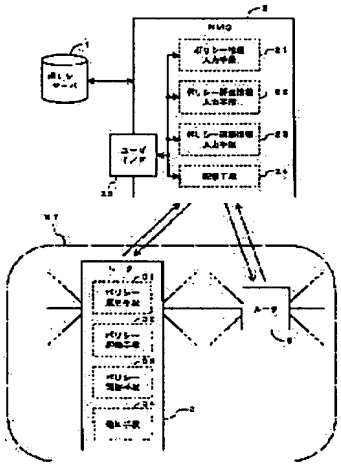
(51)Int.Cl. H04L 12/56
H04L 12/24
H04L 12/26

(21)Application number : 2000-300817
(22)Date of filing : 29.09.2000

(71)Applicant : KDDI CORP
(72)Inventor : YOSHIHARA TAKAHITO
HORIUCHI HIRONORI

(54) APPARATUS FOR MANAGING POLICY BASE MANAGING SYSTEM AND APPARATUS TO BE MANAGED

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a policy base managing system capable of optimally regulating a policy to be operated in each router (apparatus to be managed) in a network real time in response to the state of traffic.
SOLUTION: The apparatus 3 to be managed in the network NT comprises a policy operating means 31 for operating policy information delivered from the apparatus 2 for managing the policy base managing system to control the traffic, a policy evaluating means 32 for evaluating the policy during operating based on policy evaluation information delivered from the apparatus 2, and a policy evaluating means 32 for dynamically regulating the policy during the operation based on the policy regulating information delivered from the apparatus 2 and the evaluation result by the evaluating means.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－111729
（Ｐ２００２－１１１７２９Ａ）
(43)公開日　平成14年４月12日(2002.4.12)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
H04L 12/56		H04L 11/20	102　A	5K030
12/24		11/08		
12/26				

審査請求　未請求　請求項の数11　ＯＬ　（全11頁）

(21)出願番号　特願2000－300817(Ｐ2000－300817)

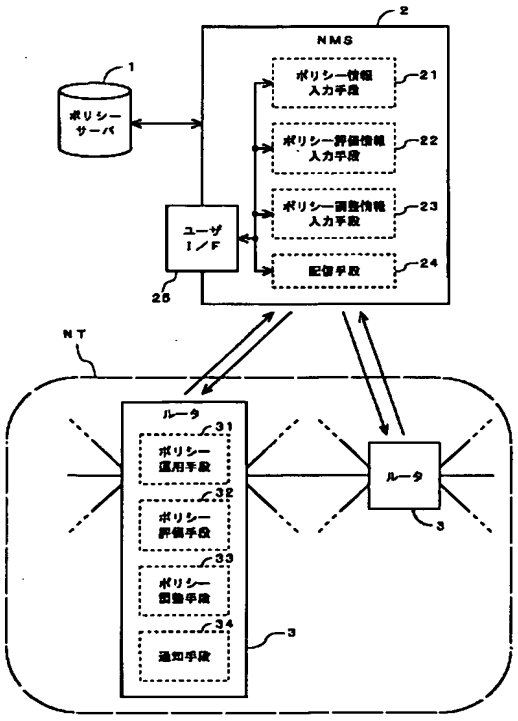
(22)出願日　平成12年９月29日(2000.9.29)

(71)出願人　000208891
ケイディーディーアイ株式会社
東京都新宿区西新宿二丁目３番２号
(72)発明者　吉原　貴仁
埼玉県上福岡市大原２－１－15　株式会社ケイディディ研究所内
(72)発明者　堀内　浩規
埼玉県上福岡市大原２－１－15　株式会社ケイディディ研究所内
(74)代理人　100084870
弁理士　田中　香樹　（外１名）

Ｆターム(参考)　5K030 GA08 GA14 HB06 HB08 JA10 KA01 KA07 LC09 LE17 MA04 MB04 MC09

(54)【発明の名称】ポリシーベース管理システムの管理装置および被管理装置

(57)【要約】
【課題】　ネットワーク内の各ルータ（被管理装置）で運用されているポリシーを、トラヒックの状況に応じて実時間で最適に調整できるようにしたポリシーベース管理システムを提供する。
【解決手段】　ネットワークＮＴ内の被管理装置３に、管理装置２から配信されたポリシー情報を運用してトラヒックを制御するポリシー運用手段３１と、管理装置２から配信されたポリシー評価情報に基づいて、運用中のポリシーを評価するポリシー評価手段３２と、管理装置２から配信されたポリシー調整情報および前記評価手段による評価結果に基づいて、運用中のポリシーを動的に調整するポリシー調整手段３３とを設けた。



1

【特許請求の範囲】

【請求項１】　ポリシー情報を管理装置で一元管理し、当該ポリシー情報を被管理装置へ配信してトラフィックを制御するポリシーベース管理システムの管理装置において、

ポリシー情報を入力するポリシー情報入力手段と、

前記被管理装置においてポリシーの適用効果を評価させるための評価情報を入力するポリシー評価情報入力手段と、

前記被管理装置で運用されるポリシーを、前記評価結果に基づいて被管理装置において動的に調整させるための調整情報を入力するポリシー調整情報入力手段と、

前記入力されたポリシー情報、ポリシー評価情報およびポリシー調整情報を前記被管理装置へ配信する配信手段とを含むことを特徴とするポリシーベース管理システムの管理装置。

【請求項２】　前記ポリシー評価情報は、各トラヒックに割り当てられたポリシーが当該トラヒックに適合しているか否かを判断させる情報を含み、

前記ポリシー調整情報は、不適合と判定されたポリシーを前記トラヒックに適合させる情報を含むことを特徴とする請求項１に記載のポリシーベース管理システムの管理装置。

【請求項３】　前記ポリシー評価情報は、運用中のポリシーが実際のトラヒックに対して資源不足であるか否かを判断させるための情報を含み、

前記ポリシー調整情報は、ポリシーの資源不足を緩和させるための情報を含むことを特徴とする請求項２に記載のポリシーベース管理システムの管理装置。

【請求項４】　前記ポリシー評価情報は、運用中のポリシーが実際のトラヒックに対して資源過剰であるか否かを判断させるための情報を含み、

前記ポリシー調整情報は、ポリシーの資源過剰を緩和させるための情報を含むことを特徴とする請求項２または３に記載のポリシーベース管理システムの管理装置。

【請求項５】　ポリシー情報を管理装置で一元管理し、当該ポリシー情報を被管理装置へ配信してトラフィックを制御するポリシーベース管理システムの被管理装置において、

前記管理装置から配信されたポリシー情報を運用してトラヒックを制御するポリシー運用手段と、

前記管理装置から配信されたポリシー評価情報に基づいて、運用中のポリシーを評価するポリシー評価手段と、

前記管理装置から配信されたポリシー調整情報および前記評価手段による評価結果に基づいて、運用中のポリシーを動的に調整するポリシー調整手段とを含むことを特徴とするポリシーベース管理システムの被管理装置。

【請求項６】　前記ポリシー評価手段は、各トラヒックに割り当てられたポリシーが当該トラヒックに適合しているか否かを評価し、

2

前記ポリシー調整手段は、前記評価手段に基づいてポリシーをトラヒックに適合させることを特徴とする請求項５に記載のポリシーベース管理システムの被管理装置。

【請求項７】　前記ポリシー調整手段は、前記評価手段により資源過剰と評価されたポリシーの品質を低下させることを特徴とする請求項６に記載のポリシーベース管理システムの被管理装置。

【請求項８】　前記ポリシー調整手段は、前記評価手段により資源不足と評価されたポリシーの品質を向上させることを特徴とする請求項６または７に記載のポリシーベース管理システムの被管理装置。

【請求項９】　前記ポリシー調整手段は、前記評価手段による評価結果に基づいて、各トラヒックに予め割り当てられているポリシーを調整することを特徴とする請求項５ないし８のいずれかに記載のポリシーベース管理システムの被管理装置。

【請求項１０】　前記調整後のポリシー情報を管理装置および他の被管理装置の少なくとも一方へ通知する通知手段をさらに具備したことを特徴とする請求項５ないし９のいずれかに記載のポリシーベース管理システムの被管理装置。

【請求項１１】　前記ポリシー調整手段は、他の被管理装置からの通知に基づいてポリシーを調整することを特徴とする請求項５ないし１０のいずれかに記載のポリシーベース管理システムの被管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ポリシー情報を管理装置で一元管理し、当該ポリシー情報をネットワーク内の被管理装置へ配信してトラフィックを制御するポリシーベース管理システムの管理装置および被管理装置に係り、特に、被管理装置においてポリシーの適用効果を評価し、この評価結果に基づいて、ポリシーをネットワークの利用状況に応じて動的に調整するようにしたポリシーベース管理システムの管理装置および被管理装置に関する。

【０００２】

【従来の技術】電子商取引や企業業務など、インターネットの商用化にともない、限られたネットワーク資源の有効利用による利潤の最大化を図るため、ユーザやアプリケーションごとに所定の通信品質（ＱｏＳ）を確保する必要性が高まっている。

【０００３】一方、このようなユーザやアプリケーションごとの通信品質を一元管理してネットワーク管理者の負担を軽減するために、ポリシーサーバにユーザやアプリケーションごとの通信品質をポリシー情報として登録し、散在するネットワーク機器にポリシーサーバからポリシー情報を配信して運用させるポリシーベース管理が普及している。このようなポリシーベース管理によれば、散在するネットワーク機器にポリシー情報を矛盾な

く設定できると共に、ポリシー情報の変更が容易になる。

【０００４】ＩＥＴＦ（Internet Engineering Task Force）で標準化が進められているインターネットの通信品質保証メカニズムの一つに、Differentiated Service（以下、DiffServと表現する）がある。ここでは、ユーザやアプリケーション毎にカスタマイズした通信品質を保証するためのポリシーが、ポリシーベース管理システムの管理装置から被管理装置へ配信されて運用される。

【０００５】図８は、DiffServ対応ネットワークの構成を示した図であり、各トラフィックには、ＱｏＳを代表する識別子としてのＰＨＢ（per-hop behavior）が割り当てられる。各ルータ９０は、入力されたトラフィックを前記ＰＨＢに応じたＱｏＳで次のルータへ転送する。なお、各ＩＰパケットには、前記ＰＨＢの代わりに６ビット長のＤＳＣＰ（Differentiated Service Code Point：通信品質情報）がＤＳ（Differentiated Service）フィールドに割り当てられ、各ルータがＰＨＢとＤＳＣＰとの対応付けを行う。

【０００６】各ルータ９０のインターフェース（Ｉ／Ｆ）は、送受信ノードに接続されるエッジＩ／Ｆ９１と他のルータに接続されるコアＩ／Ｆ９２とに区別される。前記エッジＩ／Ｆ９１はさらに、送信ノードに接続されるイングレスＩ／Ｆ９１（in）と、受信ノードに接続されるエングレスＩ／Ｆ９１（en）とに区別される。エッジＩ／Ｆ９１を備えたルータはエッジルータ９０（Ｅ）と呼ばれ、コアＩ／Ｆ９２のみのルータはコアルータ９０（Ｃ）と呼ばれる。

【０００７】上記したDiffServ対応ルータをはじめて通過するＩＰパケットは、送受信ノードのＩＰアドレスやポート番号の値に応じて、いくつかのＱｏＳクラスに分類され、エッジルータ９０（Ｅ）において、そのＤＳフィールドにＤＳＣＰ値を割り当てられる。コアルータ９０（Ｃ）は、ＤＳＣＰの値に基づいて各ＩＰパケットを分類して通信品質制御を行い、次のルータへ転送する。ＤＳＣＰの値はエッジルータ９０（Ｅ）のエングレスＩ／Ｆ９１（en）においてクリアされる。

【０００８】ＩＰパケットの分類にはクラッシファイア（classifier：分類器）が用いられる。イングレスＩ／Ｆ９１（in）のクラッシファイアはＭＦ（multi-field）クラッシファイアと呼ばれ、各ＩＰパケットを、その送受信IPアドレス、送受信ポート番号、ＩＰプロトコルバージョンの五のパラメータに基づいて分類する。コアＩ／Ｆ９２のクラッシファイアはＢＡ（Behavior Aggregate）クラッシファイアと呼ばれ、各ＩＰパケットを前記ＤＳＣＰの値で分類する。

【０００９】

【発明が解決しようとする課題】ポリシーベースに基づくネットワーク管理では、ユーザ数やネットワークトラヒックの増大、あるいは新規アプリケーションの導入といった環境変化などにより、以前に配信したポリシーが何時までも有効に機能するとは限らない。このため、既設のポリシーに対して帯域が過剰に設定されるためにネットワーク資源が無駄に消費されたり、これとは逆に、ポリシーに対して帯域が過少に設定されるために所望のサービスを提供できない場合などが生じ得る。

【００１０】したがって、ポリシーベースに基づくネットワーク管理では、(1) ポリシーの決定、(2) 決定されたポリシーの配信およびその運用、(3) 運用されているポリシーの評価、(4) 評価結果に基づくポリシーの調整、を繰り返し実時間で行うことが望ましい。

【００１１】これに対して、従来はネットワーク管理者がネットワーク上のトラヒックを常時監視し、既設のポリシーが実際のトラヒックに即していないと、その調整に必要な管理情報を別途に収集し、これに基づいてポリシーを再設定していた。しかしながら、ネットワーク環境は絶えず動的に変化するため、上記した調整方法では、ポリシーをネットワークの利用状況に応じて実時間で最適に調整することが困難であった。

【００１２】本発明の目的は、上記した従来技術の課題を解決し、ネットワーク内の各ルータで運用されているポリシーを、トラヒックの状況に応じて実時間で最適に調整できるようにしたポリシーベース管理システムの管理装置および被管理装置を提供することにある。

【００１３】

【課題を解決するための手段】上記した目的を達成するために、本発明は、ポリシー情報を管理装置で一元管理し、当該ポリシー情報を被管理装置へ配信してトラフィックを制御するポリシーベース管理システムの管理装置および被管理装置において、以下のような手段を講じた点に特徴がある。

【００１４】(1) 管理装置に、ポリシー情報を入力するポリシー情報入力手段と、前記被管理装置においてポリシーの適用効果を評価させるための評価情報を入力するポリシー評価情報入力手段と、前記被管理装置で運用されるポリシーを、前記評価結果に基づいて被管理装置において動的に調整させるための調整情報を入力するポリシー調整情報入力手段と、前記入力されたポリシー情報、ポリシー評価情報およびポリシー調整情報を前記被管理装置へ配信する配信手段とを設けた。

【００１５】(2) 被管理装置に、管理装置から配信されたポリシー情報を運用してトラヒックを制御するポリシー運用手段と、管理装置から配信されたポリシー評価情報に基づいて、運用中のポリシーを評価するポリシー評価手段と、管理装置から配信されたポリシー調整情報および前記評価手段による評価結果に基づいて、運用中のポリシーを動的に調整するポリシー調整手段とを設けた。

【００１６】上記した特徴によれば、各被管理装置に配信されて運用されているポリシーが、トラヒックの状況

に応じて動的に調整されるので、帯域などのネットワーク資源の過剰設定や過少設定が緩和されて、その有効利用が可能になる。

【００１７】

【発明の実施の形態】以下、図面を参照して本発明を詳細に説明する。図１は、本発明を適用したポリシーベース管理システムの構成を示した機能ブロック図であり、ネットワークＮＴ内でトラヒックを制御する被管理装置としての複数のルータ３と、ポリシー情報を記憶するポリシーサーバ１と、ポリシー情報を生成して各ルータ３へ配信する管理装置としてのネットワーク管理システム（ＮＭＳ）２とを含む。

【００１８】前記管理システム２は、各ルータ３において運用させるポリシーを入力するポリシー情報入力手段２１と、各ルータ３において前記ポリシーの適用効果を評価するための評価情報を入力するポリシー評価情報入力手段２２と、ルータ３で運用中のポリシーを前記評価結果に基づいて、当該ルータ３において動的に調整させるための調整情報を入力するポリシー調整情報入力手段２３と、前記入力されたポリシー情報、ポリシー評価情報およびポリシー調整情報が記述された管理スクリプトを各ルータ３へ配信する配信手段２４とを含む。

【００１９】前記ポリシー情報、ポリシー評価情報およびポリシー調整情報は、操作部および表示部等を含む適宜のマン・マシンＩ／Ｆ２５を介してオペレータにより入力することができる。

【００２０】前記各ルータ３は、前記管理システム２から配信されたポリシー情報を運用してトラヒックを制御するポリシー運用手段３１と、前記管理システム２から配信されたポリシー評価情報に基づいて、運用中のポリシーの適用効果を評価するポリシー評価手段３２と、前記管理システム２から配信されたポリシー調整情報および前記評価手段による評価結果に基づいて、運用中のポリシーを調整するポリシー調整手段３３と、調整後のポリシー情報を他のルータ３へ、管理システム２を介して間接的に、あるいは管理システム２を介さずに直接的に通知する通知手段３４とを含む。

【００２１】図２は、前記ルータ３の主要部の構成を具体的に示したブロック図であり、前記と同一の符号は同一または同等部分を表している。

【００２２】ポリシー運用手段３１において、クラッシファイア３１０１は、入力Ｉ／Ｆ３５を介して入力されたＩＰパケットを、その送信ＩＰアドレス、受信ＩＰアドレス、送信ポート番号、受信ポート番号およびＩＰプロトコルバージョンの５のパラメータに基づいて（ＭＦクラッシファイアの場合）、あるいはＤＳＣＰの値に基づいて（ＢＡクラッシファイアの場合）ＱｏＳクラスに分類する。

【００２３】ミータ３１０２、３１０３、３１０４は、ポリシー情報で予め指定された転送レートやバーストサイズにトラヒックが適合するか否かを判断し、その結果に基づいて各トラヒックの出力先を切り替える。マーカ３１０５、３１０６は、ＤＳＣＰの値を設定また置換して、当該トラフィック（またはパケット）のＱｏＳクラスを変更する。マルチプレクサ３１１１、３１１２は、複数のトラヒックをマージする。

【００２４】カウンタ３１１３～３１１７は、通過するＩＰパケット数やＩＰパケットバイト数をカウントする。無条件ドロッパ３１０７は、パケットを無条件で破棄する。選択的ドロッパ３１０８、３１０９、３１１０は、所定の条件に基づいてパケットを選択的に破棄する。キュー３１１８～３１２１は、入力されるＩＰパケットをキューイングする。スケジューラ３１３０は、前記各キュー３１１８～３１２１からＩＰパケットを所定の順序および優先度で読み出して出力Ｉ／Ｆ３６へ出力する。

【００２５】ポリシー評価手段３２の監視機能部３２１は、各カウンタ３１１３～３１１７のカウント値に基づいて、破棄されたパケット数等を検知し、運用中のポリシーの適用効果を評価する。ポリシー調整手段３３の制御機能部３３１は、前記ポリシー評価手段３２による評価結果に基づいて、運用中のポリシーを適正に調整する。通知手段３４の通知機能部３４１は、前記適用効果に関する評価結果を他のルータ３へ通知し、かつ他のルータから通知された評価結果をポリシー調整手段３３の制御機能部３３１へ通知する。制御機能部３３１は、他のルータから評価結果を通知された場合も、前記と同様に、この評価結果に基づいてポリシーを適正に調整する。

【００２６】次いで、上記した各ルータ３に対するポリシー情報、ポリシー評価情報およびポリシー調整情報の登録方法について説明する。

【００２７】本実施形態では、４種類のポリシーＡ，Ｂ，Ｃ，Ｄを、オペレータが前記管理システム２のマン・マシンＩ／Ｆ２５から登録するものとし、ポリシーＡ，Ｂ，Ｃの内容は図３に示した通りであるものとする。なお、ポリシーＤは通信品質を保証しないベストエフォート（ＢＥ）なトラヒックとして扱い、各ポリシーＡ，Ｂ，Ｃのプロファイルは、図４に示した通りであるものとする。

【００２８】図５、６、７は、管理システム２のマン・マシンＩ／Ｆ２５の操作画面上に表示されるポリシー設定画面の一例を示した図であり、それぞれポリシーＡ，Ｂ，Ｃの入力例を示している。

【００２９】ポリシー設定画面には、ポリシー情報を主に入力するポリシー情報入力領域５１と、ポリシー評価情報を主に入力する閾値設定領域５２と、ポリシー情報をルータ３において動的に調整させるためのポリシー調整情報を主に入力する自動制御設定領域５３とが用意されている。

【００３０】１．ポリシーＡの設定（図５）
①ポリシー情報の入力
ポリシーＡでは、図３に示したように、ＰＨＢ（Expedited Forwarding Per-Hop-Behavior）がＥＦ（Expedited Forwarding PHB：遅延を許容しないＱｏＳ）なので、ＥＦに対応するＤＳＣＰ（Differentiated Service Code Point：優先順位情報）の値“１０１１１０”をＤＳＣＰウインドウ５１１に登録する。
【００３１】ポリシーＡのプロファイル１では、図４に示したように、転送レート（Information Rate）閾値［Kbps］が“１００”、バーストサイズ（Burst Size）閾値［Kbytes］が“２０”なので、転送レート閾値ウインドウ５１２に“１００”、バーストサイズ閾値ウインドウ５１３に“２０”をそれぞれ登録する。
【００３２】なお、“Single Rate Three Color Marker”や“Two Rate Three Color Marker”などを用いて、パケットがプロファイルに適合するか否かを決定する場合には、さらに適用チェックボックス５１４をチェックし、Committed InformationRateウインドウ５１５およびCommitted Burst Sizeウインドウ５１６に所望の値を設定する。
【００３３】ここでは、図４に示したように、プロファイルを一つの組（転送レートおよびバーストサイズ）を使って決定する“単純トークンバケット”を採用しているため、適用チェックボックス５１４をチェックすることなく、各ウインドウ５１５、５１６は未登録のままとする。
【００３４】ＤＳＣＰの“In Profile”ウインドウ５１７には、プロファイルに適合するパケットのＤＳＣＰ値を他のＤＳＣＰ値に置換する際の値として“１０１１１０（ＥＦ）”を登録し、“Out Profile”ウインドウ５１８には、プロファイルに適合しないパケットのＤＳＣＰ値を他のＤＳＣＰ値に置換する際の値として“ｄｒｏｐ”すなわち“破棄”が登録される。
【００３５】なお、先に述べた“Single Rate Three Color Marker”や“Two Rate Three Color Marker”において、半適合と判断されたパケットのＤＳＣＰ値を他のＤＳＣＰ値に置換する際の値は、“Indeterminate”ウインドウ５１９に登録することになる。
【００３６】②ポリシー評価情報の入力
本実施形態では、運用されているポリシーの適用効果を評価するための情報として、受信パケット数、受信バイト数、廃棄パケット数などの各監視項目に関する閾値を、その監視周期と共に入力する。
【００３７】ポリシーＡでは、６０秒当たりの廃棄パケット数が１０００を超えると、閾値違反通知がポリシー調整手段３３に対して発行されものとし、“監視周期”ウインドウ５２１に６０［秒］、“破棄パケット数”ウインドウ５２２に“１０００以上”が登録される。したがって、ポリシーＡでは、６０秒間における廃棄パケット数が１０００を超えると、ポリシー調整手段３３によるポリシーの自動調整が開始されることになる。
【００３８】なお、複数の監視項目の閾値が同時に指定されている場合には、少なくとも一つの監視項目の閾値が超えた場合に通知するが、全ての監視項目の閾値が超えた場合のみ通知したり、これらの監視項目からなる論理条件式を定義して通知を発行させることも可能である。
【００３９】③ポリシー調整情報の入力
本実施形態では、前記閾値違反が通知された場合のみならず、閾値違反が通知されない場合であっても、所定の制御周期ごとに前記ポリシーの適用効果を評価してポリシーを自動調整するようにしている。
【００４０】すなわち、本実施形態では、各６０秒間の破棄パケット数が１０００を越えない限りは閾値違反とならないが、例えば６０秒間の破棄パケット数が５００程度であっても、これを救うためにはポリシーとして設定する帯域などのネットワーク資源を増やすことが望ましい。これとは逆に、破棄パケット数が０の場合には、ポリシーが品質過剰と予測されるので、当該ポリシーの品質を下げることが望ましい。
【００４１】そこで、本実施形態では所定の制御周期を設定し、当該制御周期内でのトラヒックに応じてポリシーを動的に調整するために、ネットワークの利用状況に応じた実時間でポリシーの調整を行う制御周期、調整後のポリシーＡに割り当てる転送レート、バーストサイズおよび置換するＤＳＣＰ値を指定する。
【００４２】図５の例では、現在の転送レート閾値（１００）およびバーストサイズ閾値（２０）を、直前の１２時間以内に監視された最大転送レートの１．１倍ならびに最大バーストサイズの１．０倍の値に調整するものとし、制御周期の時間ウインドウ５３１に“１２”［時間］、Peak Information Rate ウインドウ５３２に“１．１”倍、Peak Burst Size ウインドウ５３３に“１．０”倍が、それぞれ設定される。
【００４３】したがって、本実施形態のポリシーＡでは、閾値違反が発生しない場合であっても、転送レート閾値およびバーストサイズ閾値が、１２時間ごとにネットワークの利用状況に応じて動的に調整されるようになる。
【００４４】以上のようにして、各情報の設定を終了すると、“確認ボタンを”押下して当該入力操作を終了する。配信手段２４は、入力された各情報を各ルータ３へ配信する。
【００４５】２．ポリシーＢの設定（図６）
①ポリシー情報の入力
ポリシーＢでは、図３に示したように、ＰＨＢがＡＦ１１（Assured Forwarding Group：エンド・ツー・エンドでの許容パケット紛失率を小さくする）なので、ＡＦ１１に対応するＤＳＣＰの値“００１０１０”をＤＳＣＰ

ウインドウ５１１に登録する。

【００４６】ポリシーＢのプロファイル２では、図４に示したように、転送レート閾値（Information Rate）［Kbps］が“１００”、バーストサイズ閾値（Burst Size）［Kbytes］が“１００”なので、転送レート閾値ウインドウ５１２に１００、バーストサイズ閾値ウインドウ５１３に“１００”を、それぞれ登録する。なお、Committed Information RateおよびCommitted Burst Sizeの指定は前記と同様とする。

【００４７】ＤＳＣＰの“In Profile”ウインドウ５１７には、プロファイルに適合するパケットのＤＳＣＰ値を他のＤＳＣＰ値に置換する際の値として“００１０１０”（ＡＦ１１）を登録し、“Out Profile”ウインドウ５１８には、プロファイルに適合しないパケットのＤＳＣＰ値を他のＤＳＣＰ値に置換する際の値として“００１１００”（ＡＦ１２）が登録される。

【００４８】すなわち、本実施形態のポリシーＢでは、プロファイルに適合するパケットのＤＳＣＰ値は変更せず、適合しないパケットは、そのＤＳＣＰ値が“００１１００（ＡＦ１２）”に更新されて送信優先度を下げられる。

【００４９】②ポリシー評価情報の入力
ポリシーＡと同様なので、その説明は省略する。

【００５０】③ポリシー調整情報の入力
本実施形態では、制御周期の１２時間以内に閾値違反が検知されている場合（Over）は、前記転送レート閾値（ここでは、１００Kbps）を越えていない（In Profile）パケットのＤＳＣＰ値を“００１１００（ＡＦ１２）”に置換して送信優先度を下げる調整を行う。したがって、“ＤＳＣＰ”のチェックボックス５３５をチェックし、“In Profile”ウインドウ５３６に“００１１００”（ＡＦ１２）を登録する。

【００５１】なお、図６では未記入であるが、制御周期の１２時間以内に閾値違反が検知されていない場合の調整値は、“Under”以下の各欄に登録する。

【００５２】３．ポリシーＣの設定（図７）
①ポリシー情報の入力
ポリシーＣでは、図３に示したように、ＰＨＢがＡＦ１２（ＡＦ１１よりも優先度が低い）なので、ＡＦ１２に対応するＤＳＣＰの値“００１１００”をＤＳＣＰウインドウ５１１に登録する。

【００５３】ポリシーＣのプロファイル３では、図４に示したように、転送レート閾値（Information Rate）［Kbps］が“２００”、バーストサイズ閾値（Burst Size）［Kbytes］が“１００”なので、転送レート閾値ウインドウ５１２に２００、バーストサイズ閾値ウインドウ５１３に“１００”をそれぞれ登録する。なお、Committed Information RateおよびCommitted Burst Sizeの指定は前記と同様とする。

【００５４】ＤＳＣＰの“In Profile”ウインドウ５１７には、プロファイルに適合するパケットのＤＳＣＰ値を他のＤＳＣＰ値に置換する際の値として“００１１００”（ＡＦ１２）を登録し、“Out Profile”ウインドウ５１８には、プロファイルに適合しないパケットのＤＳＣＰ値を他のＤＳＣＰ値に置換する際の値として“０００００”（ＢＥ：Best Effort）が登録される。

【００５５】すなわち、本実施形態のポリシーＣでは、プロファイルに適合するパケットのＤＳＣＰ値は変更せず、適合しないパケットは、帯域制御や優先制御をまったく行わない通常のインターネットのトラフィックとして扱うように調整する。

【００５６】②ポリシー評価情報の入力
ポリシーＡ，Ｂと同様なので、その説明は省略する。

【００５７】③ポリシー調整情報の入力
本実施形態では、制御周期の１２時間以内に閾値違反が検知されている場合（Over）は、前記転送レート閾値（ここでは、２００Kbps）を越えていない（In Profile）パケットのＤＳＣＰ値を“０００００（ＢＥ）”に変更して優先制御の対象外とする。これとは逆に、制御周期の１２時間以内に閾値違反が検知されていない場合（Under）には、プロファイルに適合（In Profile）するパケットのＤＳＣＰ値を“００１０１０”（ＡＦ１１）に変更して送信優先度を上げる調整を行う。

【００５８】したがって、“ＤＳＣＰ”のチェックボックス５３５をチェックし、“Over”の“In Profile”ウインドウ５３６に“０００００”（ＢＥ）を登録し、“Under”の“In Profile”ウインドウ５３７に“００１０１０”（ＡＦ１１）を登録する。

【００５９】４．ポリシーＤの決定
ポリシーＡ，Ｂ，Ｃで決定した以外のＤＳＣＰを持つパケットは、従来のインターネットと同様に、すべてベストエフォートなトラフィックとして扱う。以降、これをポリシーＤと表現する。

【００６０】以上のようにして入力されたポリシー情報、ポリシー評価情報およびポリシー調整情報は、管理システム２の配信手段２４により、例えばＣＯＰＳ（Common Open Policy Service）、ＳＮＭＰ（Simple Network Management Protocol）、またはＣＬＩ（Command Line Interface）等のプロトコルを用いて各ルータ３へ配信される。

【００６１】各ルータ３では、ポリシー情報がポリシー運用手段３１において各ミータ３１０２、３１０３、３１０４および各マルチプレクサ３１０５、３１０６に登録され、ポリシー評価情報がポリシー評価手段３２に登録され、ポリシー調整情報はポリシー調整手段３３に登録される。

【００６２】以上のようにして、各情報の設定が終了し、ポリシー運用手段３１においてポリシーが運用されると、ポリシーＡを適用されるパケットは、クラッシファイア３１０１からミータ３１０２へ配信される。ミー

タ３１０２は、入力されたパケットの転送レートが１００［Kbps］を越えず、かつバーストサイズが２０［Kbytes］を越えない限りは、入力されたパケットを全てキュー３１１８へ転送する。キュー３１１８に蓄積されたパケットは、スケジューラ３１３０により読み出され、出力通信Ｉ／Ｆ３６を介して次段へ転送される。

【００６３】これに対して、転送レートが１００［Kbps］を越えるか、あるいはバーストサイズが２０［Kbytes］を越えると、前記ミータ３１０２は、超えた分のパケットをカウンタ３１１３へ配信する。カウンタ３１１３でカウントされたパケットは、無条件ドロッパ３１０７において全て破棄される。

【００６４】ポリシーＢを適用されるパケットは、クラッシファイア３１０１からミータ３１０３へ配信される。ミータ３１０３では、入力されたパケットの転送レートが１００［Kbps］を越えず、かつバーストサイズが１００［Kbytes］を越えない限りはマルチプレクサ３１１１へ配信し、それ以外であればマーカ３１０５へ配信する。マーカ３１０５は、そのパケットのＤＳに登録されたＤＳＣＰ値（００１０１０）を（００１１００）に変換して、その優先順位を下げる。

【００６５】マルチプレクサ３１１１は、前記ミータ３１０３およびマーカ３１０５から配信されたパケットを結合し、カウンタ３１１４を介してドロッパ３１０８へ転送する。前記ドロッパ３１０８は、キュー長が所定値よりも長くなると、それ以上のパケットを破棄する。ドロッパ３１０８で破棄されなかったパケットは、カウンタ３１１５を介してキュー３１１８へ転送される。前記カウンタ３１１４、カウンタ３１１５はドロッパ３１０８の前後でパケット数をカウントするので、両者のカウント値の差分が前記ドロッパ３１０８で破棄されたパケット数となる。

【００６６】ポリシーＣについては、ドロッパ３１０９の構成が前記ポリシーＢのドロッパ３１０８と異なり、ポリシーＣのドロッパ３１０９では前記ドロッパ３１０８よりも多くのパケットを破棄するのみで、それ以外の動作は同様なので、その説明を省略する。

【００６７】ポリシーＤを適用されるパケットは、クラッシファイア３１０１からドロッパ３１１０へ配信される。ドロッパ３１１０は、そのキュー長が所定値よりも長くなると、それ以上のパケットを破棄し、それ以外のパケットをキュー３１２１へ出力する。

【００６８】以上のようにして各ポリシーが運用されると、監視機能部３２１は、各カウンタのカウント値を、前記指定された監視周期で検知して破棄パケット数を算出し、算出結果に基づいて各ポリシーの適用効果を評価する。

【００６９】ここで、例えばポリシーＡが適用されて破棄されたパケット数をカウントするカウンタ３１１３のカウント値が“１０００”を越えると、これを制御機能部３３１へ通知してポリシーの調整を指示すと共に、通知機能部３４１を介して他のルータの制御機能部３３１へも指示する。

【００７０】制御機能部３３１は、ミータ３１０２に既登録の設定値、すなわち転送レート閾値の１００［Kbps］、バーストサイズ閾値の２０［Kbytes］を、この１２時間以内に検知された転送レートおよびバーストサイズの１．１倍、１．０倍にそれぞれ設定する。

【００７１】ここで、破棄パケットが検知されているということは、１００［Kbps］以上の転送レートおよび／または２０［Kbytes］以上のバーストサイズが検知されているはずである。したがって、前記転送レート閾値および／またはバーストサイズ閾値には、それまでよりも大きな値が設定されることになるので、ポリシーの品質が向上することになる。

【００７２】前記監視機能部３２１はさらに、閾値違反が発生しない場合であっても、前記指定された監視周期（本実施形態では、いすれのポリシーでも“１２”時間）ごとに、制御機能部３３１に対して自動制御を指示する。

【００７３】制御機能部３３１は、ミータ３１０２に既登録の設定値、すなわち転送レート閾値の１００［Kbps］、バーストサイズ閾値の２０［Kbytes］を、この１２時間以内に検知された帯域およびバーストサイズの１．１倍、１．０倍にそれぞれ設定する。

【００７４】このとき、破棄パケットが少しでも検知されている状況下では、１００［Kbps］以上の転送レートおよび／または２０［Kbytes］以上のバーストサイズが検知されているはずである。したがって、前記転送レート閾値および／またはバーストサイズ閾値には、それまでよりも大きな値が設定されるので、ポリシーの品質が向上し、品質不足が緩和されることになる。

【００７５】これに対して、破棄パケットが検知されていなければ、１００［Kbps］以上の転送レートおよび２０［Kbytes］以上のバーストサイズが検知されていないので、前記転送レート閾値およびバーストサイズ閾値には、それまでよりも小さな値が設定されることになる。したがって、ポリシーの品質が現在よりも低下して品質過剰が緩和されることになる。

【００７６】なお、他のポリシーＢ，Ｃ，Ｄの動作は、上記したポリシーＡに関する動作説明から明らかなので、その説明は省略する。

【００７７】上記した実施形態では、本発明をDiffServへ適用した場合を例にして説明したが、本発明はこれのみに限定されるものではなく、ＩＥＴＦやＤＭＴＦが標準化を積極的に進めている“Integrated Service”（通称Intserv ）にも同様に適用することができる。また、主にパケットの送信優先制御や帯域制御を行うポリシーベース管理のみならず、ユーザや会社組織、ホストや端末、ならびにアプリケーションごとにカスタマイズした

13

アクセス制御を行うファイアウォールを用いたポリシーベースのネットワーク管理にも、同様に適用できる。

【００７８】

【発明の効果】本発明によれば、以下のような効果が達成される。

【００７９】(1) 各被管理装置（ルータ）に配信されて運用されているポリシーが、トラヒックの状況に応じて動的に調整されるので、通信品質の過剰や不足が緩和されてネットワーク資源の有効利用が可能になる。

【００８０】(2) 一つの被管理装置におけるポリシーの調整内容が他の被管理装置にも反映されるので、ポリシー調整の実効が得られる。

【図面の簡単な説明】

【図１】　本発明を適用したポリシーベース管理システムの構成を示した機能ブロック図である。

【図２】　被管理装置としてのルータの主要部の構成を示したブロック図である。

【図３】　各ポリシーＡ，Ｂ，Ｃの内容を模式的に表現した図である。

14

【図４】　各プロファイルの内容を模式的に表現した図である。

【図５】　ポリシーＡを設定する際のポリシー入力画面の表示例を示した図である。

【図６】　ポリシーＢを設定する際のポリシー入力画面の表示例を示した図である。

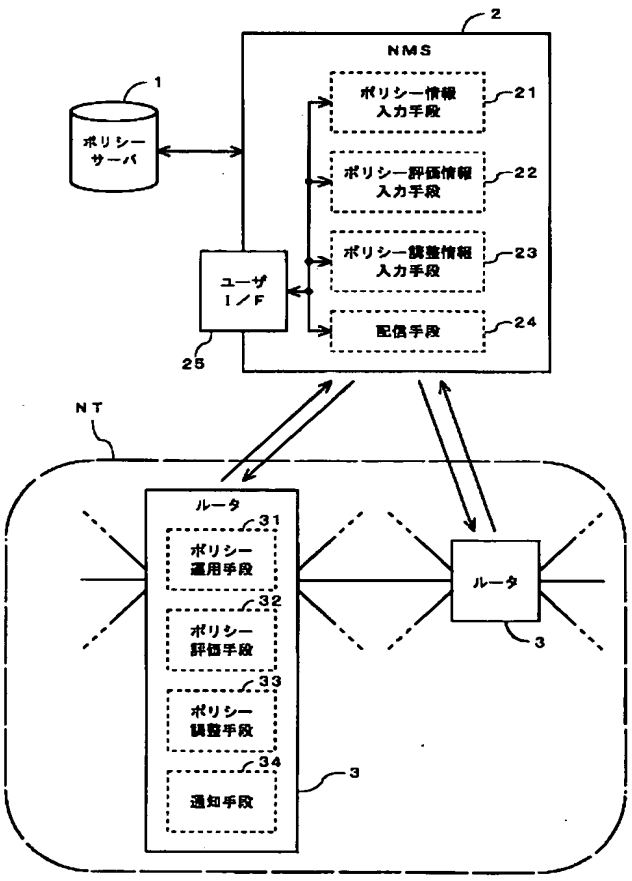
【図７】　ポリシーＣを設定する際のポリシー入力画面の表示例を示した図である。

【図８】　DiffServ対応ネットワークの構成を示した図である。

【符号の説明】

ポリシーサーバ１…，２…ネットワーク管理システム，３…ルータ，２１…ポリシー情報入力手段，２２…ポリシー評価情報入力手段，２３…ポリシー調整情報入力手段，２４…配信手段，２５…マン・マシンＩ／Ｆ，３１…ポリシー運用手段，３２…ポリシー評価手段，３３…ポリシー調整手段，３４…通知手段

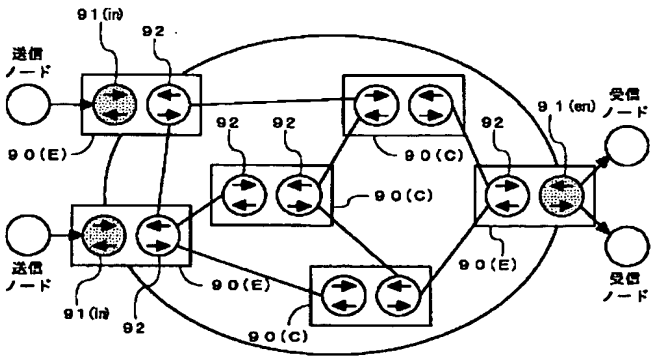
【図１】



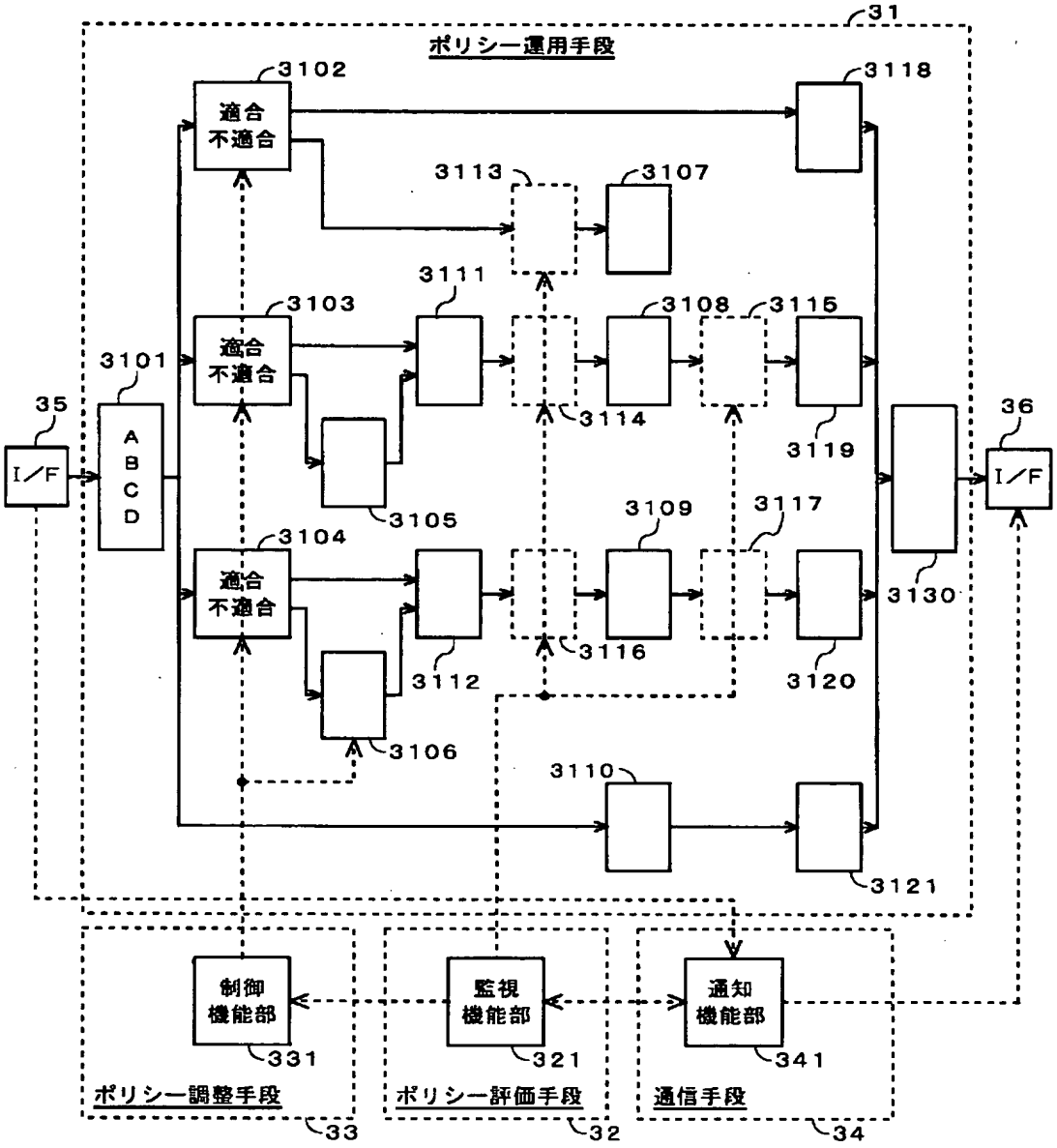
【図３】

ポリシーＩＤ	ＤＳＣＰ	ＰＨＢ	プロファイル	制御方法
A	101110	ＥＦ	Profile1	プロファイルに適合しないものを破棄。
B	001010	ＡＦ11	Profile2	プロファイルに適合しないものをマーキング。キューが溢れた場合、キューの最後のパケットを破棄。
C	001100	ＡＦ12	Profile3	プロファイルに適合しないものをマーキング。キューが溢れた場合、キューの最後のパケットを破棄。

【図８】



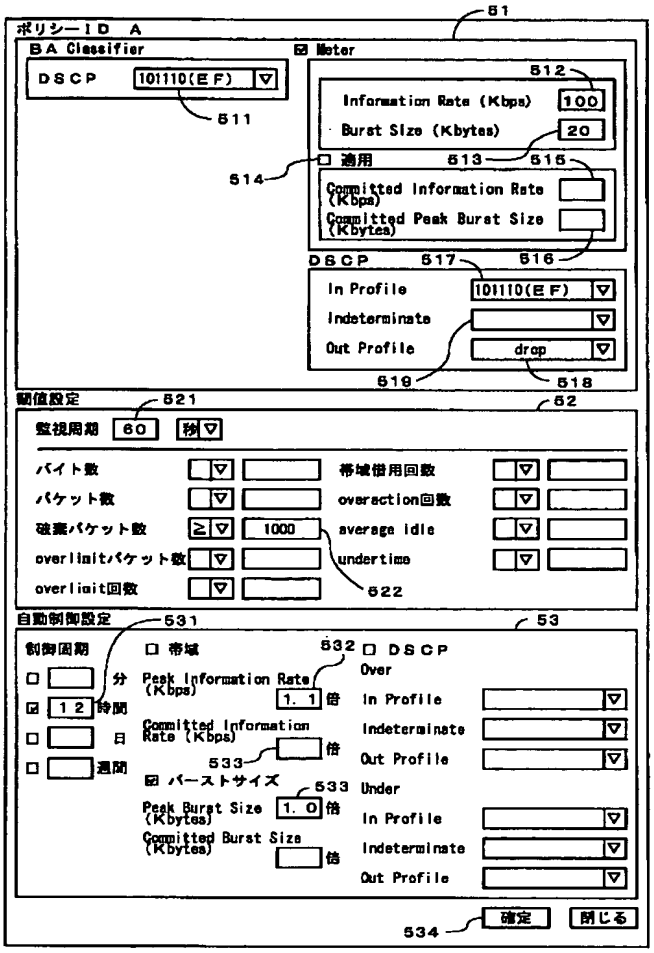
【図２】



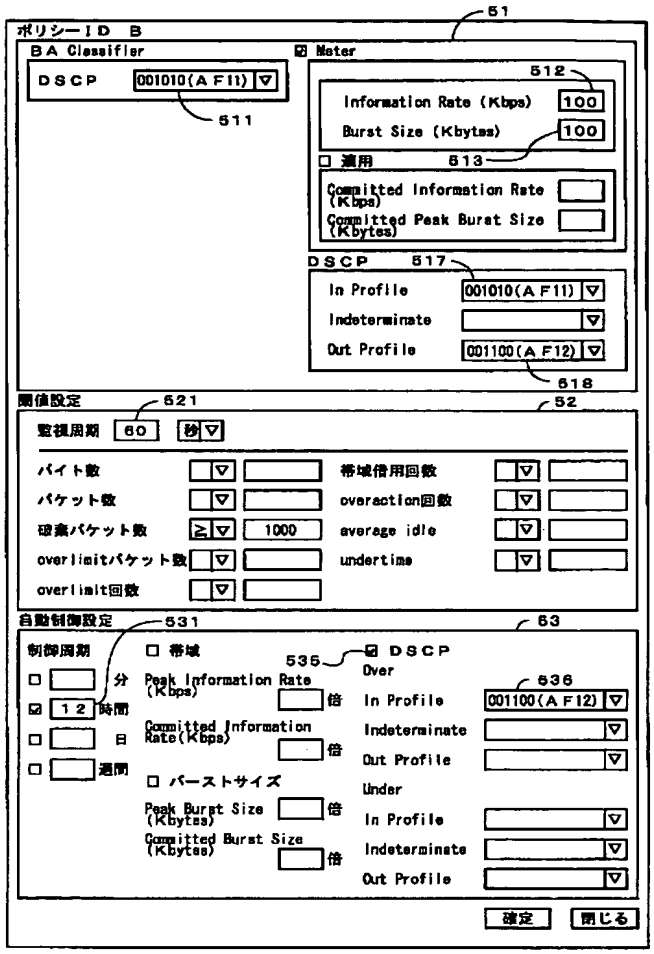
【図４】

	Ｔｙｐｅ	転送レート（Kbps）	バーストサイズ（Kbytes）
Profile1	単純トークンパケット	１００	２０
Profile2	単純トークンパケット	１００	１００
Profile3	単純トークンパケット	２００	１００

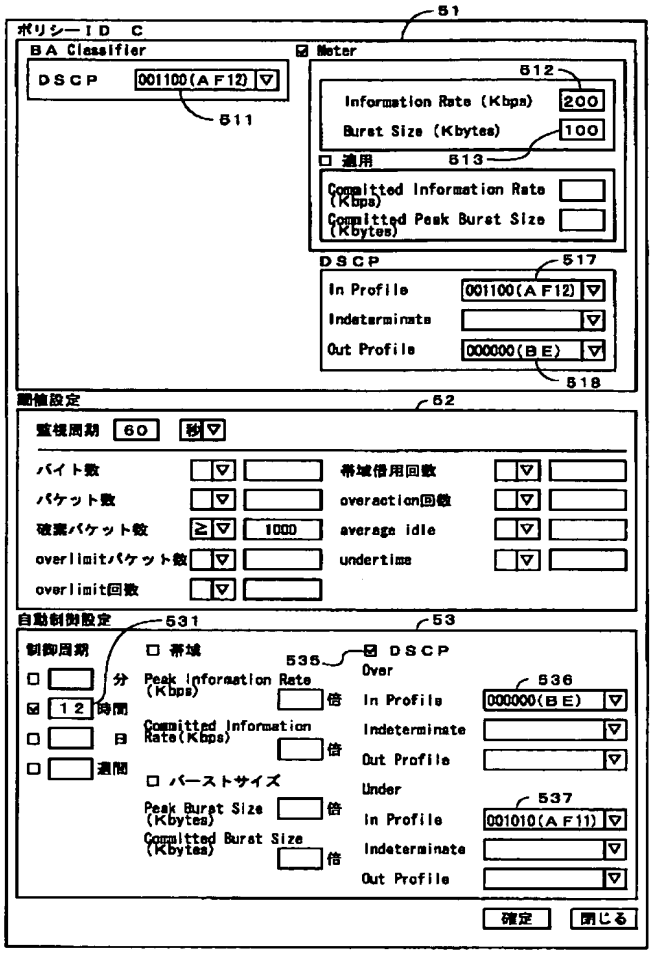
【図５】


ポリシーＩＤ　Ａ
51
BA Classifier
DSCP
101110(ＥＦ)
511
Meter
512
Information Rate (Kbps)
100
Burst Size (Kbytes)
20
適用
513
514
515
Committed Information Rate (Kbps)
Committed Peak Burst Size (Kbytes)
DSCP
517
516
In Profile
101110(ＥＦ)
Indeterminate
Out Profile
drop
519
518
閾値設定
521
52
監視周期
60
秒
バイト数
パケット数
破棄パケット数
≧
1000
overlimitパケット数
overlimit回数
帯域借用回数
overaction回数
average idle
undertime
522
自動制御設定
531
53
制御周期
分
12
時間
日
週間
帯域
532
Peak Information Rate (Kbps)
1.1
倍
Committed Information Rate (Kbps)
533
バーストサイズ
Peak Burst Size (Kbytes)
1.0
Committed Burst Size (Kbytes)
DSCP
Over
In Profile
Indeterminate
Out Profile
Under
534
確定
閉じる

【図６】


ポリシーＩＤ　Ｂ
51
BA Classifier
DSCP
001010(ＡＦ11)
511
Meter
512
Information Rate (Kbps)
100
Burst Size (Kbytes)
100
適用
513
Committed Information Rate (Kbps)
Committed Peak Burst Size (Kbytes)
DSCP
517
In Profile
001010(ＡＦ11)
Indeterminate
Out Profile
001100(ＡＦ12)
518
閾値設定
521
52
監視周期
60
秒
バイト数
パケット数
破棄パケット数
≧
1000
overlimitパケット数
overlimit回数
帯域借用回数
overaction回数
average idle
undertime
自動制御設定
531
53
制御周期
分
12
時間
日
週間
帯域
Peak Information Rate (Kbps)
535
Committed Information Rate (Kbps)
バーストサイズ
Peak Burst Size (Kbytes)
Committed Burst Size (Kbytes)
DSCP
Over
536
In Profile
001100(ＡＦ12)
Indeterminate
Out Profile
Under
確定
閉じる

【図７】


51
ポリシーＩＤ　C
BA Classifier
DSCP
001100(AF12)
511
Meter
512
Information Rate (Kbps)
200
Burst Size (Kbytes)
100
適用
513
Committed Information Rate (Kbps)
Committed Peak Burst Size (Kbytes)
DSCP
517
In Profile
001100(AF12)
Indeterminate
Out Profile
000000(BE)
518
動作設定
52
監視周期
60
秒
バイト数
パケット数
破棄パケット数
≧
1000
overlimitパケット数
overlimit回数
帯域借用回数
overaction回数
average idle
undertime
自動制御設定
531
53
制御周期
分
12
時間
日
週間
帯域
Peak Information Rate (Kbps)
倍
535
Committed Information Rate(Kbps)
倍
バーストサイズ
Peak Burst Size (Kbytes)
倍
Committed Burst Size (Kbytes)
倍
DSCP
Over
In Profile
000000(BE)
536
Indeterminate
Out Profile
Under
537
In Profile
001010(AF11)
Indeterminate
Out Profile
確定
閉じる